NOW AVAILABLE:

FEATURED RESOURCES:

REALTIME COMMUNITIES

- Messaging and Web Security
- Unified Communications
- Vista
- Windows Server

NEWSLETTER

Email Address:

Subscribe

MONTHLY ARCHIVES

- January 2008
- December 2007
- November 2007
- October 2007
- September 2007

« Don't Expect Privacy At The Iowa Caucuses | Main | The Iowa Caucus Experience in Madison County: Cameras Not a Factor »

More On Überveillance And Privacy

I recently blogged about "6 "Scary Stuff" Privacy Terms IT, Info Sec and Privacy Folks Should Know."

I was very pleasantly surprised to hear from Dr. Michael G. Michael and his wife Dr. Katina Michael a couple of days ago about the post! (Thank you Michael and Katina!) They provided some additional very interesting information about the term "Überveillance." With their permission, here is a large portion of the message they sent to me:

> "I am writing regarding your posting: "6 "Scary Stuff" Privacy Terms IT, Info Sec and Privacy Folks Should Know" dated November 27, 2007.
> First, thank you for including the term uberveillance in your list.
>
> My husband and I thought you might be interested in some specific definitions/citations which might shed light on the overall meaning of the term.
>
> Basic definition of Uberveillance:
>
> "Überveillance is an above and beyond, an exaggerated, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on" but "always with you" (it is ubiquitous) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that omnipresence in the 'material' world will not always equate with omniscience, hence the real concern for misinformation, misinterpretation, and information manipulation.
>
> Rebecca, in a nutshell, think of it in the following way: whereas Big Brother is on the outside looking down, uberveillance is on the inside looking out. Consequently, the all important social implications are demonstrably, far more extensive and culture altering than what Orwell had himself imagined."
>
> OTHER SOURCES:
> Primary source on Uberveillance (Oct, 2007): "A note on Uberveillance": http://ro.uow.edu.au/infopapers/560/
>
> First conference citation on Uberveillance (July, 2006): "The Emerging Ethics of Humancentric GPS Tracking and Monitoring": http://ro.uow.edu.au/infopapers/385/

» August 2007
Complete Archive

RSS
» FEEDBURNER
» PODCAST
» iTUNES

ASK THE EXPERT
Have a question for our resident expert? Email your questions to Rebecca.

First journal citation on Uberveillance (Dec, 2006): “National Security: The Social Implications of the Politics of Transparency”: http://ro.uow.edu.au/infopapers/390/

Another relevant source where Uberveillance is cited and described by other academics/practitioners:
http://www.uow.edu.au/~katina/rnsa07.htm
http://www.homelandsecurity.org.au/publications.html#SocialImplications07_proceedi
http://www.anu.edu.au/people/Roger.Clarke/DV/RNSA07.html"

I found the papers written by the Drs. very interesting and informative.

Of note, I found the paper "The Emerging Ethics of Humancentric GPS Tracking and Monitoring" particularly thought-provoking.

A family member very close to me suffered 12 long excruciatingly painful years from Alzheimers, and such tracking devices were very important for ensuring her safety, so I was interested to see what they wrote with regard to that kind of situation.

There certainly are many differing ethical considerations for a wide variety of situations where GPS and RFID tracking could, or have been, used. Some completely inappropriate and quite concerning.

As I communicated with the Drs. Michael, regarding technologies, or other concepts, for that matter, for identifying specific individuals, it seems many often leach out into areas where they were never meant to go. Beyond technologies, just look at the U.S. and the use of the social security number...it has become something completely different than what it ever was intended to be when it was created. The unintended uses have resulted in growing numbers of fraud and identity theft, in addition to other unsavory activities.

The GPS and RFID trackers can be used for great good in ensuring the safety of those who are not able to make decisions for themselves, but they can also be used for very egregious privacy invasions, such as forcing all employees to get RFID implants to keep track of their location. However, some states (California, Wisconsin and North Dakota) have passed laws prohibiting companies from forcing employees to get these types of tracking devices.

Tags: ambient technology awareness and training Dr. Katina Michael Dr. Michael G. Michael employee privacy employee tracking GPS tracking information security IT compliance policies and procedures privacy privacy law RFID risk management security awareness security training social security number SSN uberveillance

Posted by Rebecca Herold on January 3, 2008 10:50 AM | Permalink

TrackBack

TrackBack URL for this entry:
http://www.realtime-itcompliance.com/type/mt-tb.cgi/617

Post a comment

(All comments are approved by site leader before appearing here. Thanks for commenting!)

- Don't Expect Privacy At The Iowa Caucuses
- UK Imposes Record Fine of $2.54 Million Against Life Insurance Company For Poor Information Security & Privacy Practices
- New U.S. Law Effective Jan 1 Prohibits Lithium Batteries In Checked Luggage
- FTC Behavioral Advertising Privacy Principles: Give Them Your Feedback!
- FTC Fines Mortgage Co. For Tossing PII Into Dumpster: FACTA/FCRA, GLBA, & FTC Act Violations
- 3 Inspiring Examples For This Season of Holidays
- Be Prepared For Privacy Breaches!
- The 12 Threats of Chistmas

Name:

Email Address:

URL:

Remember personal info?

Comments: (you may use HTML tags for style)

Preview Post

CATEGORIES

- Government
- Identity theft
- Information Security
- Laws & Regulations
- Lost & Stolen Laptops
- Miscellaneous
- Non-compliance Sanctions Examples
- Podcast
- Privacy Incidents
- Privacy and Compliance
- Training & awareness

LATEST WHITE PAPERS

- Policy and IT Controls Compliance Challenges and Solutions
- Creating Scalable, Repeatable, and Sustainable Infrastructure Controls Assessment
- The Essential Elements of Comprehensive Endpoint Security
- Improving IT Compliance: Guidance for Midsize Organizations
- Network Access Control Technologies and Symantec Compliance on Contact
- Using Security Compliance Software to Improve Business Efficiency and Reduce Costs
- Debunking the Top 5 Myths of Compliance

REBECCA HEROLD'S BIO:

Rebecca Herold, CISSP, CIPP, CISA, CISM, FLMI, has over 16 years of experience as an information technology and information security, privacy and compliance professional. Rebecca created the Information Protect program at Principal Financial Group where she worke for 12 years. Rebecca has authored 10 books to date, many book chapters and dozens of articles, and is an adjunct professor for the Norwich University Master of Science in Information Assurance (MSIA) program. Yo can contact Rebecca at: rebecca_herold@realtimepublishers.net